UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PURE POWER BOOT CAMP, INC.
PURE POWER BOOT-CAMP FRANCHISING CORPORATION, and PURE POWER BOOT CAMP JERICHO INC.,

Plaintiffs,

- against –

WARRIOR FITNESS BOOT CAMP, LLC; ALEXANDER KENNETH FELL a/k/a ALEX FELL, Individually; RUBEN DARIO BELLIARD a/k/a RUBEN BELLIARD, Individually; JENNIFER J. LEE, Individually; and NANCY BAYNARD, Individually,

Defendants.

ECF Case
Case No. 08-cv-4810 (JGK) (THK)

DEFENDANTS' REPLY MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION FOR AN ORDER PRECLUDING THE USE OR DISCLOSURE OF SPECIFIC E-MAILS ILLEGALLY OBTAINED BY PLAINTIFFS, DIRECTING THE IMMEDIATE RETURN OF THE E-MAILS, AND GRANTING DEFENDANTS THEIR ATTORNEY'S FEES, COSTS, AND DISBURSEMENTS RESULTING FROM PLAINTIFFS' ILLEGAL ACTIONS

Carolyn D. Richmond (CR 7946)
Daniel A. Schnapp, Esq. (DS 3484)
Eli Z. Freedberg, Esq. (EF 6854)
FOX ROTHSCHILD LLP
100 Park Avenue, 15th Floor
New York, NY 10017
Tel: (212) 878-7900
Fax: (212) 692-0940

Defendants respectfully submit this Reply Memorandum of Law in support of its Motion for an Order Precluding the Use or Disclosure of Specific E-mails Illegally Obtained by Plaintiffs, directing the immediate return of the e-mails, and granting Defendants their attorney's fees, costs, and disbursements resulting from Plaintiffs' illegal actions.

PRELIMINARY STATEMENT

Defendants instituted this Motion because Plaintiffs stole confidential and privileged emails from three of Defendants' private email accounts. Plaintiffs never provided Defendants with a corporate (Pure Power) email address and none of the emails stolen by Plaintiffs are emails that were sent from a Pure Power email address or were sent or received while Defendants were "on the clock" at Plaintiffs' business. In fact, all of the emails were stolen after Defendants Fell and Belliard were no longer in Plaintiffs' employ.

In their opposition to the Motion, Plaintiffs do not dispute that:

(1) all of the emails were stolen *after* Defendants no longer worked for Plaintiffs;

(2) the emails were stolen from *three* of Defendants' email accounts and that at no time were any passwords made available for Defendants' Warrior Fitness and Gmail accounts;

(3) Plaintiffs obtained and used Defendant Fell's password for his Hotmail account without any explicit authorization;

(4) Plaintiffs subsequently *read, downloaded, printed, and read* the private emails from all three accounts in public;

(5) Plaintiffs removed the times and dates of the emails, resulting in sanctionable spoliation of evidence.

Ultimately, Plaintiffs' failure to address certain of Defendants' arguments reflects the same sort of arrogance that lies behind Plaintiffs' belief that they are not accountable for the theft of the emails in the first place. Indeed, Plaintiffs' opposition papers make clear that Plaintiffs feel no need to justify—or even explain—their actions.

Plaintiffs must be held accountable. Accordingly, the use or disclosure of these e-mails must be precluded by this Court, and Plaintiffs must be directed to immediately return the e-mails, and to reimburse Defendants for the legal fees they have expended on this motion.

FACTS[1]

Plaintiffs and their principal, Lauren Brenner ("Brenner") hacked into, and stole emails that were not written, sent, or received on Plaintiffs' computers.

As Plaintiffs' concede, all of these stolen emails were drafted on Defendants' *own home or WFBC corporate* computers or wireless devices while Defendants were not working at Plaintiffs' facility. As Plaintiffs also concede, most of these emails were transmitted or received after Fell's and Belliard's employment with Plaintiffs had already ended.

Plaintiffs only address Fell's Hotmail Account in their opposition and do not dispute Defendants' allegations that Plaintiffs stole emails from Fell's Gmail Account and the corporate Warrior Account. Accordingly, Plaintiffs concede that these emails from the Gmail and Warrior accounts were in fact stolen and, as a result, the use of these emails must be completely barred in this litigation.

Plaintiffs do admit that they used Fell's Hotmail passwords, and argue only that they were given "implied consent" to access these Hotmail emails. Aside from the fact that at no time did Fell disclose such passwords to Plaintiffs, Plaintiffs chose to ignore the fact that they accessed these emails *after* Fell no longer worked for Plaintiffs, and that Plaintiffs illegally read, downloaded, printed, and read these emails in public.

Plaintiffs argue that they somehow have the right to access these email communications because Fell once used Plaintiffs' computer in contravention of Plaintiffs' alleged workplace policy. Assuming that this policy even existed during the relevant time period, which is highly

[1] For a complete review of the facts pertinent to this motion, and for a description of the stolen emails, Defendants respectfully refer the Court to the Affidavit of Alexander Kenneth Fell and the Memorandum of law submitted in support of Defendants' Motion.

suspect, such a policy cannot confer a permanent and irrevocable right to access the private email accounts of an employee regardless of where or when the emails were drafted. The alleged policy certainly does not survive post-employment.

Plaintiffs also misappropriated several emails that constitute attorney-client communications. Plaintiffs now argue that these emails are not privileged because Fell waived the privilege. In fact, no such waiver occurred because every recipient of every challenged email was being simultaneously represented by counsel and these communication were intended to further the representation.

Lastly, Plaintiffs do not even attempt to deny the obvious evidence of their spoliation of the emails.

ARGUMENT

POINT I

PLAINTIFFS MUST BE PRECLUDED FROM THE USE OR DISCLOSURE OF THE STOLEN E-MAILS

A. Plaintiffs Accessed All of The E-Mails in Violation of the Electronic Communications Privacy Act

At the same time that Plaintiffs concede that they removed the time and date that they accessed and printed out the stolen emails, Plaintiffs claim that the Electronic Communications Privacy Act ("ECPA") is inapplicable because the theft of Fell's emails did not occur contemporaneously with the transmission of the emails.

Although we cannot know the precise moment when Plaintiffs stole all of the emails, since Plaintiffs have removed the time and date from the emails, at a minimum it is clear that the majority of emails were initially transmitted or received in March and April 2008, immediately prior to the time that Plaintiffs filed this action and their Motion for a Preliminary Injunction (to which Plaintiffs attached the stolen emails as exhibits).

In addition, Plaintiffs state that they were in possession of Fell's passwords for his Hotmail accounts. Plaintiffs were therefore able to monitor the emails from this account and steal the emails contemporaneously with their transmission. Plaintiffs cannot escape the inexorable conclusion that their interceptions of the emails was contemporaneous.

As a result, Plaintiff's argument that the ECPA is inapplicable must fail.

B. Plaintiffs Accessed All of The E-Mails in Violation of the Stored Communications Act

Plaintiffs argue that there can be no violation of the Stored Communications Act ("SCA") because Fell allegedly consented, at least impliedly, to Plaintiffs' monitoring of his emails. Plaintiffs' argument is based upon their contention that: (1) Plaintiffs maintained a corporate policy allowing the employer to monitor electronic transmissions, (2) Fell left his email account name and password stored on Plaintiffs' computers, (3) Fell accessed Plaintiffs' computers in violation of Plaintiffs' policy forbidding personal use of the computers, and (4) Plaintiffs were within their rights to hack into Fell's emails once it discovered Fell's purported misconduct.

Plaintiffs, however, apparently want the Court to ignore the fact that, even if the alleged corporate policy existed, such a policy no longer applied once Fell stopped working at Plaintiffs' gyms and Plaintiffs' espionage continued.

The cases cited by Plaintiffs in support of the proposition that they were entitled to spy on Fell and steal his emails are inapposite. All of the cases involve scenarios where employees argued that the subject emails were sent using the email addresses or servers provided to them by their employer and/or the emails were sent during the time the employee was working for the employer.

For example, in *Scott v. Beth Israel Med. Ctr.*, 17 Misc.3d 934, 936, 847 N.Y.S.2d 436 (Sup. Ct., NY Co. 2007), a doctor sent email using his work email address over his employer's email server. Similarly, in *Long v. Marubeni Am. Corp.*, 2006 WL 2998671, at *3 (S.D.N.Y.

2006), plaintiffs used their employer's computer while at work to send letters to their counsel. In *US v. Rittweger*, 258, F.Supp.2d 345, 347 (S.D.N.Y. 2003), an employee who was at work placed phone calls that were intercepted and recorded. In *US v. Workman*, 80 F.3d 688, 692 (2d Cir. 1996), a prisoner placed telephone calls using a prison's telephone system.

Here, Fell has testified and Plaintiffs do not dispute that the intercepted emails were sent on Fell's personal Hotmail, Gmail and WFBC Accounts, while Fell was not at work and not using Plaintiffs' computers. Fell could not have sent the majority of the emails while working for Plaintiffs because most of the emails at issue were written or sent to him after his employment with Plaintiffs had already terminated. In fact, Fell has testified that these emails were sent or received by him on his own time and on his own personal computers. For the emails that were sent or received during the time period Fell was working for Plaintiffs, these emails could not have been written while Fell was at work since they bear time stamps from the early hours of the morning when Plaintiffs' gym was closed.

1. This Court Has Broad Discretion to Fashion a Remedy Precluding the Use of the Emails

Plaintiffs mistakenly rely on the case of *Fayemi v. Hambrecht and Quist, Inc.*, 174 F.R.D. 319, 324 (S.D.N.Y. 1997) in support of their argument that the sanction should not be the complete preclusion of the misappropriated emails, even if Plaintiffs violated federal law in obtaining the emails. In *Fayemi*, the Court recognized that courts necessarily have the inherent equitable power to govern discovery in order to prevent abuses, oppression and injustices, such as those committed by Plaintiffs in the case at bar. In fact, Justice Francis of this Court presented the following hypothetical:

> Suppose a plaintiff burglarized a defendant's premises and secured privileged documents. Could one seriously contend that a court could not prohibit the use of those documents in the proceeding before it simply because the documents were not obtained through the discovery process.

Id.

The facts here mirror the hypothetical posed by the *Fayemi* court and, here, as in *Fayemi,* the Court has the inherent authority to fashion a sanction against a party who attempts to use in litigation material improperly obtained outside of the discovery process. In other words, broad sanctions are appropriate because Plaintiffs have violated federal and state eavesdropping laws in order to hack into and steal Defendants' private and confidential emails.

C. Plaintiffs Have Abandoned the Right to Enforce Their Purported Policy Forbidding the Use of Computers

Even if Plaintiffs did in fact maintain the disputed corporate policy forbidding use of Plaintiffs' computers for personal use, an allegation which Defendants vigorously deny, the policy was rendered unenforceable because it was routinely ignored and Plaintiffs failed to take any acts to enforce the policy. *See Fundamental Portfolio Advisors, Inc. v. Tocqueville Asset Management, L.P.,* 7 N.Y.3d 96, 104 (N.Y. Ct. App. 2004) (contractual rights may be abandoned by failure to act).

Here, Brenner's assistant, Elizabeth Lorenzi testified under oath that Plaintiffs maintained a policy forbidding use of emails but that "Fell would use the computer on many occasions." *See* Aff. Of Elizabeth Lorenzi, sworn to on July 10, 2008, ¶ 5. Plaintiffs' failure to enforce this policy on the "many occasions" on which the computer were used for personal purposes renders the policy moot and Plaintiffs may not now use the terms of the policy to justify their interception of and theft of Fell's emails.

D. Plaintiffs Accessed All of The E-Mails in Violation of New York State Law and this Law Does not Require Contemporaneous Interception

As Defendants pointed out in their Motion, under New York State law, the contents of recorded communications, or evidence derived therefrom, which have been obtained by conduct constituting the crime of eavesdropping cannot be received in evidence in any trial, hearing or proceeding before any court. CPLR § 4506. A person is guilty of eavesdropping when she

unlawfully engages in wiretapping, mechanical overhearing of a conversation, or intercepting or accessing of an electronic communication. N.Y. Penal Law § 250.05.

In their opposition, Plaintiffs argue, incorrectly, that New York law requires the interception of the electronic communication to occur at the same time as the initial transmission. In fact, the New York statute, makes no such provision. Plaintiffs base their disingenuous argument on the federal statute which does not have any actual place in the New York statute. Realizing that their argument will fail, Plaintiffs feebly offer that the Court may "find otherwise." *See* Plaintiffs' Memorandum of Law at pp. 6-7.

In any event, CPLR § 4506 mandates the preclusion and return of the emails.

E. "E-Mails #12-14" and "E-Mail #28" Are Also Protected by Attorney-Client Privilege and Cannot be Used or Disclosed

Plaintiffs argue that emails sent from a law firm's paralegal's to the law firm's clients are not privileged. Plaintiffs also argue that emails shared between two parties simultaneously represented by counsel causes waiver of the attorney-client privilege. Plaintiffs also argue that a lawyer's communication to a client concerning the status of a filing with a state administrative agency are not privileged. All of these arguments are wrong.

"E-mail #13" and "E-mail # 14" are protected by the attorney-client privilege. These e-mail were confidential communications consisting of correspondence related to the status of registering the client's company to do business in the state of New York.

Moreover, the protection was not waived in any manner, because the e-mail was not disclosed to a person not represented by counsel at anytime--notwithstanding Plaintiffs' illegally accessing the communication. As a result, the communication is afforded the attorney-client protection and the emails must be precluded from use or disclosure.

Finally, because these e-mails are privileged documents, Plaintiffs would not otherwise have had access to them through discovery. The privileged nature of these e-mails means that

Defendants would not have had to turn them over to Plaintiffs, and as a result, the only way that Plaintiffs were able to access the e-mails, and their contents was through illegal, and nefarious means that violated Defendants' legal rights, their absolute expectation of privacy, and breached their-attorney client privilege.

F. All of the E-Mails Must be Also Precluded Due to their Spoliation

Spoliation is the destruction, significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending, or reasonably foreseeable litigation. *West v. Goodyear Tire & Rubber Co.,* 167 F.3d 776, 779 (2d Cir. 1999).

Here, Plaintiffs have altered the print outs of Fell's emails by deleting the "time-stamp" that appears at the bottom of every document every time someone prints out an email in a transparent attempt to cover up their theft and misappropriation. Plaintiffs never deny altering these documents. Rather they attempt to downplay their wrongdoing by stating that this behavior does not constitute spoliation because Defendants are unable to show that emails with relevant dates exist. We suppose that Plaintiffs want the Court to ignore Fell's affidavit submitted in support of Defendants' Motion which attaches true and correct copies of the emails showing the time and date they were printed out.

Moreover, Plaintiffs disingenuously argue that the dates of the emails are unimportant. As set forth above, the dates are in fact highly relevant because they will establish that Plaintiffs were engaged in a contemporaneous theft of the emails, a fact which should result in severe sanctions against Plaintiffs.

Consequently, Defendants have demonstrated that Plaintiffs committed spoliation by altering the emails.

CONCLUSION

Plaintiffs have failed to even attempt to counter the majority of Defendants' arguments. Plaintiffs have committed theft but have not even tried to justify or explain their actions. Accordingly, Defendants respectfully urge this Court to grant their Motion in its entirety.

Dated: July 15, 2008
New York, NY

Carolyn D. Richmond (CR-7946)
Daniel A. Schnapp (DS-3484)
Eli Z. Freedberg (EF-6854)
Fox Rothschild LLP
Attorneys for Defendants
100 Park Avenue
Suite 1500
New York, NY 10017
Direct (212) 878-7960
Fax (212) 692-0940